UNIVERSITI PUTRA MALAYSIA

BEBERAPA PENGGUNAAN TEORI NOMBOR DALAM KRIPTOGRAFI

FARIDAH BINTI YUNOS

FSAS 2001 55

BEBERAPA PENGGUNAAN TEORI NOMBOR DALAM KRIPTOGRAFI

FARIDAH BINTI YUNOS

MASTER SAINS
UNIVERSITI PUTRA MALAYSIA
2001

BEBERAPA PENGGUNAAN TEORI NOMBOR DALAM KRIPTOGRAFI

Oleh

FARIDAH BINTI YUNOS

Tesis ini Dikemukakan Sebagai Memenuhi Keperluan Untuk Ijazah Master Sains Di Fakulti Sains dan Pengajian Alam Sekitar Universiti Putra Malaysia

Februari 2001

Ingatan Tulus Ikhlas buat

Safiah Marjan

Mohd Ishak Yunos

Pawziah Yunos

Salmah Yunos

Siti Zaleha Yunos

Siti Zabedah Yunos

'Sesungguhnya yang baik itu datangnya dari Allah, dan yang buruk itu adalah dari kelemahan saya sendiri'

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Master Sains.

BEBERAPA PENGGUNAAN TEORI NOMBOR DALAM KRIPTOGRAFI

Oleh

FARIDAH BINTI YUNOS

Februari 2001

Pengerusi : Dr. Mohamad Rushdan bin Md Said

Fakulti : Fakulti Sains dan Pengajian Alam Sekitar

Penyelidikan yang dilakukan meliputi penggunaan Teori Nombor dalam bidang kriptografi. Melalui penggunaan konsep aritmetik modulo, beberapa kaedah pengkriptanan dibangunkan berorientasikan sistem Saifer Digrafik, RSA (Ron Rivest, Adi Shamir dan Leonard Adleman) dan LUC (fungsi Lucas jadi semula linear berdarjah dua) . Ketiga-tiga kaedah tersebut dikaji dan berasaskan teknik tersebut, kaedah baru dibina. Berdasarkan algoritma pengkriptanan yang dibina, suatu kaedah penghuraian diperkenalkan. Keberkesanan teknik yang dibangunkan ini diilustrasikan melalui beberapa contoh. Terdapat tiga bahagian utama yang dibincangkan dalam tesis ini.

Pada bahagian pertama, kajian ini menyelidiki kelemahan yang wujud dalam sistem Saifer Digrafik $C_{2\times j} \equiv A_{2\times 2} P_{2\times j} \ (mod\ 26)$ terutamanya di segi analisis kekerapan huruf teks saifer dan analisis kunci pengkriptan.

Kajian ini dimulai dengan meneliti dua pembahagi sepunya terbesar bagi penentu matriks pengkriptan, $|A_{2\times2}|$ dan 26. Pengkriptanan mesej dilanjutkan kepada transformasi dwifungsi, trifungsi seterusnya pengitlakannya menghasilkan transformasi Pengkriptanan Polifungsi Saifer Digrafik bermodulo 26 dengan mengkategorikannya kepada dua kunci pengkriptan iaitu kunci pengkriptan sama dan kunci pengkriptan berbeza pada setiap transformasi. Berlandaskan teknik yang sama dan berkonsepkan sistem pemecahan nombor-nombor bersepadan dalam teks asal kepada beberapa digit tertentu, penerokaan diperluaskan lagi kepada sistem Pengkriptanan Polifungsi Saifer digrafik bermodulo suatu integer positif N_1. Kajian ini juga menerangkan mekanisma penyimpanan kunci rahsia bersifat simetri yang mungkin diperlukan oleh sistem Polifungsi Saifer Digrafik dengan kunci pengkriptan berbeza pada setiap transformasi.

Di bahagian kedua, bertitik tolak daripada transformasi LUC dengan fungsi jadi semula linear berdarjah dua

$$V_n(P,Q) \equiv PV_{n-1}(P,Q) - QV_{n-2}(P,Q) \bmod N$$

dan $U_n(P,Q) \equiv PU_{n-1}(P,Q) - QU_{n-2}(P,Q) \bmod N$ dengan pendekatan $Q=1$, sistem LUC dikembangkan lagi sehingga penghantaran mesej melalui transformasi polifungsi. Penyelidikan ini membuktikan bahawa fungsi Lehmer Totient $S(N)$ sentiasa sama pada setiap transformasi bagi membolehkan perlaksanaan penghuraian mesej saifer.

Bahagian ketiga pula membentangkan kaedah gabungan sistem RSA-Digrafik dan Digrafik-LUC. Kedua-dua sistem ini memperbaiki kelemahan sistem Saifer Digrafik yang terdahulu. Kajian ini turut mencadangkan gabungan LUC-RSA untuk menghindarkan cubaan mengesan mesej asal dengan Teorem Baki Cina dalam sistem RSA.

Untuk setiap sistem kriptografi yang dibangunkan, kajian ini juga menentukan syarat mesej asal tidak menyamai mesej saifer.

Abstract of thesis submitted to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Master of Science.

SOME APPLICATIONS OF NUMBER THEORY TO CRYPTOGRAPHY

By

FARIDAH BINTI YUNOS

February 2001

Chairman : Dr. Mohamad Rushdan bin Md Said

Faculty : Faculty of Science and Environmental Studies

This research investigates some applications of Number Theory to Cryptography. Based on the modulo arithmetic concept, a number of encryption methods are developed by employing the Cypher Diagraphic, RSA (Ron Rivest, Adi Shamir and Leonard Adleman) and LUC (second order linear reccurence Lucas function) systems as our tools. All the three systems are studied and based on them a new system is developed. Based on the new encryption algorithm developed, a new method of decrypting messages is introduced. Some illustrations will be given to demonstrate the effectiveness. There are three main parts to this thesis.

In the first part, this research investigates the weaknesses in the Cypher Digraphic system $C_{2\times j} \equiv A_{2\times 2} P_{2\times j} \ (mod\ 26)$ especially in the analysis of cyphertext frequency and encrypting key. This research begins by looking at two greatest common divisors for the determinant of the encrypting matrix,

$|A_{2\times 2}|$ and 26. The message encryption is extended to bifunction and trifunction transformations and generally the Cypher Diagraphic Polyfunction Encryption with modulo 26 which is categorised into two keys which are the similar encrypting key and the different encrypting key at each transformation. Based on the similar technique and the concept of splitting the numbers in plaintext into some specific digits, this research extend the investigation to Cypher Diagraphic Polyfunction Encryption for positive integer modulo N_1. This research also explains the mechanism of symmetry secret key storing which are possibly needed in Cypher Diagraphic Polyfunction system with different encrypting key for every transformation.

In the second part, by the concept of LUC transformation in the second order linear reccurence function

$$V_n(P,Q) \equiv PV_{n-1}(P,Q) - QV_{n-2}(P,Q) \bmod N$$

and $U_n(P,Q) \equiv PU_{n-1}(P,Q) - QU_{n-2}(P,Q) \bmod N$

with $Q = 1$, the LUC system is extended to sending of messages via polyfunction transformation. This research shows that the Lehmer Totient Function $S(N)$ is always the same in each transformation to enable us to carry out the decryption process.

In the third part, the RSA-Diagraphic and Diagraphic-LUC cryptosystems are presented. Both of them improve the effectiveness of the Cypher Diagraphic system. This research also proposes the use of LUC-RSA

combination system to prevent decyphering of the original message through the use of Chinese Remainder Theorem in the RSA system.

For each cryptographic system that is developed, it must be ensured that the conditions for the plaintext are not similar to that of the cyphertext.

PENGHARGAAN

Segala pujian dan sanjungan untuk Allah, Tuhan seru sekalian alam ini. Alhamdulillah, dengan limpah rahmat-Nya penulis dapat menyempurnakan kajian ini. Juga, selawat dan salam ke atas junjungan besar Nabi Muhammad (S.A.W).

Jutaan terima kasih diucapkan kepada Pengerusi Jawatankuasa Penyeliaan iaitu Dr. Mohamad Rushdan bin Md Said atas segala kesabaran, dorongan dan bimbingan beliau selama beberapa tahun ini. Ucapan terima kasih yang tak terhingga diberikan kepada Prof. Dr. Kamel Ariffin bin Mohd Atan atas segala nasihat yang sungguh bermakna.

Ribuan terima kasih juga diucapkan kepada Prof Madya Dr. Harun bin Budin selaku Jawatankuasa Penasihat yang turut sama memberikan idea di awal kajian ini.

Tidak lupa kepada rakan-rakan daripada Pusat Pengajian Matrikulasi dan Jabatan Matematik UPM yang memberikan dorongan secara tak langsung. Akhir sekali, ingatan buat ibu yang sentiasa mendoakan kebahagiaan anaknya di sini.

Saya mengesahkan bahawa Jawatankuasa Pemeriksa bagi Faridah bt. Yunos telah mengadakan pemeriksaan akhir pada 5hb. Februari, 2001 untuk menilai tesis Master Sains beliau yang bertajuk "Beberapa Penggunaan Teori Nombor Dalam Kriptografi" mengikut Akta Universiti Pertanian Malaysia (Ijazah Lanjutan) 1980 dan Peraturan-peraturan Universiti Pertanian Malaysia (Ijazah lanjutan) 1981. Jawatankuasa pemeriksa memperakukan bahawa calon ini layak dianugerahkan ijazah tersebut. Anggota Jawatankuasa Pemeriksa adalah seperti berikut:

Peng Yee Hock, Ph.D.
Fakulti Sains dan Pengajian Alam Sekitar
Universiti Putra Malaysia
(Pengerusi)

Mohd Rushdan Md. Said, Ph.D.
Fakulti Sains dan Pengajian Alam Sekitar
Universiti Putra Malaysia
(Ahli)

Kamel Ariffin Mohd Atan, Ph.D.
Fakulti Sains dan Pengajian Alam Sekitar
Universiti Putra Malaysia
(Ahli)

Haji Harun Budin, Ph.D.
Fakulti Sains dan Pengajian Alam Sekitar
Universiti Putra Malaysia
(Ahli)

MOHD GHAZALI MOHAYIDIN, Ph.D.
Profesor
Timbalan Dekan Pengajian Siswazah
Universiti Putra Malaysia

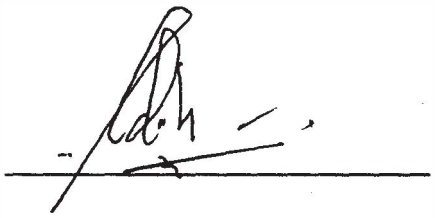
Tarikh : 27 MAR 2001

Tesis ini telah diserahkan kepada Senat Universiti Putra Malaysia dan telah diterima sebagai memenuhi keperluan untuk Ijazah Master Sains.

KAMIS AWANG, Ph.D.
Profesor Madya
Dekan Pusat Pengajian Siswazah
Universiti Putra Malaysia

Tarikh :

Saya mengaku bahawa tesis ini adalah hasil kerja saya yang asli melainkan petikan dan sedutan yang telah diberikan penghargaan di dalam tesis. Saya juga mengaku bahawa tesis ini tidak dimajukan untuk ijazah-ijazah lain di Universiti Putra Malaysia atau institusi-institusi lain.



Faridah binti Yunos

Tarikh : 22/03/01

ISI KANDUNGAN

SENARAI JADUAL

Jadual **Mukasurat**

SENARAI GAMBARAJAH

Gambarajah **Mukasurat**

SENARAI SIMBOL DAN SINGKATAN

mod	modulo
adj	adjoin
g.s.k	gandaan sepunya terkecil
log	logaritma
eks	fungsi eksponen
$\equiv$	kongruen
$\not\equiv$	bukan kongruen
$\prod$	hasil darab

BAB 1

PENGENALAN

1.1 Sejarah Ringkas

Semenjak zaman dahulu, penghantaran mesej secara rahsia adalah penting dalam hal ehwal ketenteraan, hubungan antarabangsa dan perdagangan. Perkembangan terkini sistem komunikasi meningkatkan lagi kepentingannya terutama dalam urusan kewangan dan perbankan. Bidang kajian penulisan mesej rahsia ini dinamakan kriptologi sementara seni sains dalam merekabentuk penulisan mesej rahsia ini dinamai kriptografi. Ukiran yang dipahat pada batu oleh orang Mesir purba 1900 S.M disenaraikan sebagai rekabentuk penulisan mesej terawal (lihat [5] m/s71). Suatu ketika dahulu iaitu pada 50-60 S.M, Julius Caeser telah menggunakan kaedah anjakan huruf-huruf mesej asal dan juga transliterasi huruf-huruf Latin kepada Greek atau kepada satu nombor rahsia yang bersesuaian (lihat [5] m/s 83). Idea penulisan mesej rahsia telah diterajui oleh pengkaji-pengkaji lain dan tidak ketinggalan pada tahun 855, seorang pemikir Islam iaitu Abu Bakr Ahmad ben 'Ali ben Wahshiyya an-Nabati telah memperkenalkan beberapa abjad rahsia yang dipercayai boleh digunakan dalam silap mata (lihat [5] m/s 93). Sekitar tahun 1300 an, ahli Matematik Islam terkenal iaitu 'Abd al-Rahman Ibn Khaldun menulis dalam bukunya 'Al-Muqaddimah', suatu

kajian tentang penggunaan nama-nama wangian, buah-buahan, burung dan bunga yang boleh dikaitkan dengan huruf-huruf (lihat [5] m/s 94).

Melalui penggunaan konsep dalam Teori Nombor, beberapa kaedah kriptografi telah dapat dibangunkan oleh pengkaji-pengkaji terdahulu dan kaedah pengungkapan mesej ini telah ditingkatkan mutu keselamatannya dari masa ke semasa . Perbincangan ini adalah mengenai kajian yang telah dibuat semenjak tahun 1970 an yang berasaskan aritmetik modulo. Perlu diingat bahawa , penghantaran mesej berasaskan aritmetik modulo ini sebenarnya telah digunakan oleh Julius Caeser suatu ketika dahulu.

Kajian terawal dibuat dengan menukarkan abjad standard antarabangsa $A, B, C, \ldots, Z$ kepada nombor-nombor integer bersepadan iaitu $0,1,2,\ldots,25$. Misalnya mesej 'R A H S I A' diutuskan kepada individu tertentu dalam bentuk kod rahsia '17 0 7 18 8 0'. Sistem ini terlalu mudah sehinggakan individu lain boleh mengenalpasti mesej sebenar hanya dengan congakan sahaja. Kajian telah dilanjutkan kepada kaedah transformasi anjakan $C \equiv P + k (mod\, 26)$ (lihat Bahagian 1.3 dan [10] m/s 209-211), seterusnya kaedah perutusan mesej yang lebih umum daripada itu iaitu transformasi afin $C \equiv aP + b (mod\, 26)$ (lihat Bahagian 1.4 dan [10] m/s 211). Kajian kemudiannya merupakan pengubahsuaian kaedah transformasi afin kepada sistem yang lebih praktikal dengan menggunakan operasi matriks. Berkonsepkan teknik penulisan mesej yang telah dibangunkan oleh Lester S

Hill (lihat [5] m/s 404) pada tahun 1929 ini dan berasaskan aritmetik modulo, dua sistem kriptografi dibina menggunakan transformasi Saifer Digrafik $C_{2\times1} \equiv A_{2\times2}P_{2\times1}\,(mod\,26)$ (lihat Bahagian 1.5.1 dan [10] m/s 218) dan transformasi Saifer Poligrafik $C_{i\times j} \equiv A_{i\times i}P_{i\times j}\,(mod\,26)$ (lihat Bahagian 1.5.2 dan [10] m/s 219).

Dalam tahun 1976, Whitfield Diffie dan Martin Hellman daripada Stanford University (lihat [12] m/s 1) telah memperkenalkan sistem bereksponen untuk menghantar mesej rahsia yang kemudiannya idea ini direalisasikan dalam sistem RSA oleh Ron Rivest, Adi Shamir dan Leonard Adleman [9] pada tahun 1978. Sistem penghantaran mesej berdasarkan modulo bereksponen ini juga dipercayai telah digunakan oleh Pohlig dan Hellman dalam tahun 1978 (lihat [10] m/s 224). Pohlig dan Hellman menggunakan padanan huruf A,B,C,...,Y,Z dengan nombor-nombor sepadan 00,01,02,...,24,25. Dalam sistem RSA, mesej rahsia diperolehi dengan rumus $C \equiv P^e\,(mod\,N)$ (lihat Bahagian 1.6 dan [10] m/s 230). Pelbagai kaedah lain bagi memperbaiki kelemahan yang ada termasuklah sistem ELGAMAL pada tahun 1985 (lihat [7] m/s 294) dan yang agak terkini sistem LUC $C \equiv V_e(P,1)\,mod\,N$ (lihat Bahagian 1.7) yang diilhamkan oleh Peter Smith [14] pada tahun 1991. Pengubahsuaian telah dibuat terhadap sistem kriptografi yang ada dengan merekabentuk gabungan dua sistem misalnya pada tahun 1994, LUCELG dan LUCDIFF telah dibangunkan (lihat [7] m/s 316).

Perbincangan di sini menjurus kepada kaedah transformasi anjakan, transformasi afin, transformasi Saifer Digrafik, transformasi Poligrafik, RSA dan LUC masing-masing akan diperincikan dalam Bahagian 1.3, 1.4, 1.5.1, 1.5.2, 1.6 dan 1.7.

1.2 Beberapa Istilah, Tata-tanda Dan Takrif

Sebelum perbincangan ini dilanjutkan, beberapa istilah yang biasa digunakan dalam sistem kriptografi diperjelaskan maksudnya seperti berikut:

1) Teks asal : mesej yang akan diubah oleh pengutus mesej kepada bentuk mesej rahsia.

2) Teks saifer : teks rahsia yang akan diutuskan kepada penerima mesej.

3) Pengkriptanan : proses menukarkan teks asal kepada teks saifer.

4) Penghuraian : proses menukarkan teks saifer kepada teks asal.

5) Kunci rahsia : nombor atau jujukan nombor-nombor integer yang dirahsiakan daripada pengetahuan umum.

6) Kunci awam : nombor atau jujukan nombor-nombor integer yang diketahui umum.

7) Kunci pengkriptan : kunci rahsia/awam yang diaplikasikan semasa proses pengkriptanan.

8) Kunci penghurai : kunci rahsia/awam yang diaplikasikan semasa proses penghuraian.

Berikut merupakan beberapa tata-tanda yang digunakan dalam kajian kita.

P merupakan nombor bersepadan dalam teks asal. Contohnya, jika nombor bersepadan bagi teks asal abjad R ialah 17 maka $P = 17$.

$P_{i\times j} = [p_{xy}]$ merupakan jujukan nombor-nombor bersepadan dengan teks asal iaitu p_{xy} bagi setiap $x \le i$ dan $y \le j$ yang disusun mengikut tertib matriks baris ke-i lajur ke-j. Contohnya, jujukan nombor-nombor bersepadan teks asal $B \quad A \quad H \quad A \quad Y \quad A$ iaitu $1 \quad 0 \quad 7 \quad 0 \quad 24 \quad 0$ disusun mengikut matriks 3 baris 2 lajur menjadi $P_{3\times 2} = \begin{bmatrix} 1 & 0 \\ 0 & 24 \\ 7 & 0 \end{bmatrix}$.

P_r merupakan nombor-nombor bersepadan bagi setiap blok ke-r dalam teks asal dengan $r = 1,2,3,\ldots$.Contohnya, katakan mesej asal terdiri daripada 3 blok dengan setiap blok mengandungi 2 digit.

Blok 1 : 54

Blok 2 : 65

Blok 3 : 78

Jadi, $P_1 = 54$, $P_2 = 65$ dan $P_3 = 78$.